була б його смерть.

В даному випадку бажано для фіксації крім протоколу використовувати диктофон. Також потрібно негайно встановити у очевидців прикмети і дані зовнішності нападників, їх кількість, в якому напрямку і на якому транспорті вони зникли.

Не зважаючи на значну кількість проведення початкових слідчих дій та тактичних операцій, все ж таки деякі недоліки початкового етапу розслідування вбивств, вчинених на замовлення з'ясовуються, на жаль, тільки в ході судового розгляду.

Якщо в ході досудового слідства не до кінця з'ясовані окремі обставини, то відповідні прогалини використовуються підсудними та їх захисниками для заперечування кваліфікації скоєного. Більш того, саме в процесі судового розгляду надається зовсім інша оцінка одних і тих же обставин, в результаті чого змінюється кваліфікація злочину.

Підсумовуючи вищезазначене, можна констатувати, що успіх в розслідуванні вбивств, вчинених на замовлення, залежить від наступних чинників:

1. Правильне обрання загального алгоритму пошукових дій слідчого на початковому етапі розслідування, знання основних особливостей типових слідчих ситуацій та версій.

2. Висування і паралельна перевірка всіх можливих версій.

3. Забезпечення проведення первинного комплексу слідчих і оперативних дій по всім зазначеним напрямкам.

4. Своєчасність висунення і перевірка самої версії про вчинення вбивства на замовлення - у випадках, коли замовний характер злочину на початковому етапі розслідування ще не є очевидним.

5. Своєчасне вжиття заходів щодо запобігання знищення доказів і збору достатньої кількості непрямих доказів, в тому числі тих, які вказують на мотив вчиненого злочину.

Література

1. Кримінально-процесуальний кодекс України від 13.04.2012 р. №4651-VI / [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws

2. Комиссаров В.И. Особенности расследования убийств, совершённых по найму / В.И. Комиссаров, О.В. Булаева. – М.: Издательство "Юрлитинформ", 2010. – 160 с.

3. Бородулин А. И. Убийства по найму: криминалистическая характеристика и методика расследования / Под редакцией профессора Р.С. Белкина. – М.: "Новый Юрист" 1997. – 162 с.

4. Тіщенко В.В. Теоретичні і практичні основи методики розслідування злочинів. - Одеса : Фенікс, 2007. - 260 с.

5. Саінчин О. С. Слідчі ситуації та алгоритми дій в методиці розслідування серійних вбивств / О.С. Саінчин. - Актуальні проблеми держави і права. – 2007. – № 22. - С. 49 -55.

6. Саінчин О.С. Криміналістична структура приватних криміналістичних методик розслідування умисних вбивств / О.С. Саінчин. – Науковий вісник Херсонського державного університету. – 2013. – Випуск 4. Т.2. – С. 153-156.

7. Жерж Н.А. Початковий етап розслідування вбивств, вчинених в умовах неочевидності / Н. А. Жерж. - Актуальні проблеми держави і права. – 2014. – № 63. - С. 406 - 412.

8. Алексійчук В. І. Огляд місця події : тактика і психологія : моногр. / В. І. Алексійчук. – Х. : Вид. агенція "Апостіль", 2011. – 190 с.

9. Мироненко С.Ю. Взаємодія оперативних працівників і слідчих при розслідуванні вбивств на замовлення: проблеми та шляхи вирішення / Мироненко С.Ю. – Південноукраїнський правничий часопис. – 2009. - № 3. – С. 182-186.

10. Журавель В.А. Криміналістичні методики: сучасні наукові концепції / В.А. Журавель - Х. : Вид. агенція "Апостіль", 2012. - 304 с.

11. Тіщенко В.В. Криміналістичні технології в теорії і практиці розслідування / / Актуальні проблеми держави і права. / Збірник наукових праць. - Вип. 44. - Одеса : Юридична література, 2008. - С. 18 - 24.

12. Торган Л. Криминалистичесие проблемы исследования инсценировок как способов противодействия расследованию преступлений [Текст] / Л. Торган // Международный научно–практический правовой журнал "Legea si Viata" 2013. – № 4. – С. 206–209.

13. Костенко М.В. Вбивство на замовлення: криміналістична характеристика: Монографія. – Харків, 2006. – 159 с.

14. Коновалова В.Е. Убийство: искусство расследования: Монография. – Харьков: Факт, 2001. – 220 с.

Крижановська О.В.,
викладач кафедри адміністративної
діяльності ОВС та економічної безпеки
ОДУВС
Надійшла до редакції: 13.11.2015

УДК 342.951

ЗАБЕЗПЕЧЕННЯ ПРИРОДНО-ТЕХНОГЕННОЇ БЕЗПЕКИ В УКРАЇНІ І ПРОБЛЕМА ВИЗНАЧЕННЯ ПОНЯТТЯ "КРИТИЧНА ІНФРАСТРУКТУРА"

Курбанов Я. Л.

У статті розкривається зміст поняття "критична інфраструктура", розглядаються проблеми вдосконалення системи гарантування техногенної безпеки населення і території України, підвищення надійності та безпеки функціонування життєво важливих для країни об'єктів критичної інфраструктури.

***Ключові слова**: критична інфраструктура, природно-техногенна безпека, надзвичайна ситуація.*

В статье раскрывается содержание понятия "критическая инфраструктура", рассматриваются проблемы усовершенствования системы обеспечения техногенной безопасности населения и территории Украины, повышения надежности и безопасности функционирования жизненно важных для страны объектов критической инфраструктуры.

***Ключевые слова**: критическая инфраструктура, природно-техногенная безопасность, чрезвычайная ситуация.*

Keywords: critical infrastructure,

Високі темпи розвитку техногенної сфери та підвищення ролі людського фактора в ній стали причинами багатьох природних і техногенних катастроф у XX и XXI століттях. Людство, дедалі більше втручаючись в природне середовище і змінюючи його відповідно до своїх безмежних потреб, залишається відносно безпорадним перед руйнівним впливом великомасштабних надзвичайних ситуацій техногенного характеру, які стають наслідком на аварій на об'єктах, втрата або порушення нормального функціонування яких призведе до значних або навіть непоправних негативних наслідків для національної безпеки.

Сьогодні актуальною проблемою є вдосконалення системи гарантування безпеки населення і території України з поступовим підвищенням рівня техногенної безпеки в державі до рівня розвинених країн світу, підвищення надійності та безпеки функціонування життєво важливих для країни об'єктів критичної інфраструктури, і в першу чергу на територіях, що зазнають суттєвого антропогенного впливу, який призвів до значних негативних екологічно небезпечних змін природного ландшафту, тобто на техногенно навантажених територіях. Такі території характеризуються високою ймовірністю виходу з адміністративно-правового режиму повсякденного функціонування окремих територіальних підсистем єдиної державної системи цивільного захисту.

Учасники Міжнародної науково-практичної конференції "Актуальні проблеми моделювання ризиків і загроз виникнення надзвичайних ситуацій на об'єктах критичної інфраструктури", яка відбулася 20–21 квітня 2015 р. у м. Київ, констатували, що рівень забезпечення природно-техногенної безпеки та захисту об'єктів критичної інфраструктури в Україні не відповідає вимогам сьогодення, а ризики та загрози перевищують як нормативні, так і аналогічні значення абсолютної більшості зарубіжних країн. Особливий наголос робився і на протидії та запобіганні терористичним загрозам в умовах сучасних викликів сьогодення.

Питання захисту критичної інфраструктури, методології ідентифікації об'єктів критичної інфраструктури присвячено роботи фахівців Національного інституту стратегічних досліджень Д.С.Бірюкова та С.І.Кондратова [1; 2].

Сьогодні відсутність чіткого визначення терміна "критична інфраструктура" в українському законодавстві і, як наслідок, відсутність переліку об'єктів такої категорії створюють перешкоду для ефективного виконання п. 6 рішення Ради національної безпеки і оборони України від 1 березня 2014 р. "Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України" (введеного в дію указом Президента України № 189/2014 від 02.03.2014 р.), згідно з яким Міністерству внутрішніх справ України наказується забезпечити "посилену охорону об'єктів енергетики та критичної інфраструктури".

Термін "критична інфраструктура" увійшов в обіг ділового, наукового та дипломатичного спілкування з середини 1990-х рр., і спочатку був пов'язаний з інформаційною інфраструктурою.

Питання про впорядкування термінології в галузі гарантування безпеки при надзвичайних ситуаціях на порядок денний поставлено тільки останнім часом. На даний момент у цій сфері відсутній єдиний методологічний підхід до розуміння тих чи інших дефініцій у царині різних аспектів гарантування безпеки при надзвичайних ситуаціях.

Разом із тим єдиний, якісний термінологічний апарат зумовлює можливість уніфікованого підходу до розуміння проблем гарантування безпеки при надзвичайних ситуаціях, необхідного для подальшого розвитку й удосконалення законодавства та іншого нормативно-правового регулювання в даній сфері суспільних відносин. Суперечливість, некомплексність, а часто й відсутність необхідної легальної термінології породжують значні проблеми як із точки зору ефективності юридичної техніки при розробленні нормативної бази запобігання й ліквідації надзвичайних ситуацій, так і з точки зору правозастосовної практики. Причому найважливіша правозастосовна проблема полягає в точній кваліфікації надзвичайної ситуації, яка повинна визначати економічні механізми у сфері зниження ризиків і пом'якшення наслідків надзвичайних ситуацій, включаючи компенсаційні витрати на відновлення порушеного економічного потенціалу постраждалої території, проведення екологічних заходів, надання допомоги постраждалому населенню, забезпечення публічного порядку. Але найважливішим є те, що точна юридична кваліфікація надзвичайної ситуації на об'єктах критичної інфраструктури повинна визначати всю стратегію дій уповноважених юридичних і посадових осіб, а також стратегію поведінки правоохоронних органів і населення в зоні ймовірної надзвичайної ситуації.

Стандартне визначення критичної інфраструктури передбачає галузі економіки і технологічні системи, вразливі і водночас життєво важливі для безпеки й стабільного функціонування суспільства. Це перш за все транспорт, енергетика, водопостачання, хімічне та біологічне виробництва, основні системи зв'язку і комунікацій. Дестабілізація, не кажучи вже про колапс, цих систем обертається важкими, а за найгіршого сценарію – і катастрофічними наслідками для сучасного суспільства, економіки та держави. В умовах глобальної економіки і сучасного динамічного інформаційного суспільства поняття "критичність інфраструктури" стає більш відносним. За винятком громадського транспорту, ряду особливо небезпечних виробництв, системи постачання питної води і деяких інших галузей, дійсно дедалі важче визначити, які саме ресурси мають найбільш "критичне" значення. В умовах зростання глобальної взаємозалежності і оптимізації виробництва практично будь-яка інфраструктура, включаючи, наприклад, рутинне виробництво досить стандартних товарів або матеріалів, може за певних умов виявитися "критичною" - до такої міри, що локальна аварія або тимчасовий колапс може раптово обернутися глобальною дестабілізацією цілої галузі. Нерідко реальний ступінь "критичності" того чи іншого елемента інфраструктури з'ясовується вже після того, як стався такого роду колапс.

Під критичною інфраструктурою військові фахівці розуміють об'єкти інфраструктури держави, вихід із ладу яких (або їх знищення) може спричинити катастрофічні наслідки в галузі безпеки і оборони, економіки, охорони здоров'я тощо, констатуючи, що цілісна система захисту об'єктів критичної інфраструктури в Україні відсутня, як і нормативне визначення терміна "критична інфраструктура" [3].

У цілому концепція критичної інфраструктури була сформована та розроблена у США. Терористичні акти 11

вересня 2001 р. спонукали уряд кардинальним чином переглянути не тільки своє уявлення про систему безпеки держави і суспільства за нових геополітичних умов, але й внести зміни в законодавство, структуру уряду, державний бюджет, пріоритети основних напрямів внутрішньої і зовнішньої політики. У США критична інфраструктура визначається як "сукупність фізичних або віртуальних систем і засобів, важливих для США такою мірою, що їх вихід із ладу або знищення можуть призвести до згубних наслідків у галузі оборони, економіки, охорони здоров'я та безпеки нації" [4].

Виклики щодо безпеки критичної інфраструктури не вичерпуються проблемами визначення порівняльної "критичності" тієї чи іншої інфраструктури. Із низки важливих дилем у цій галузі визначимо такі. Національна або міжнародна відповідальність? Відповідальність за гарантування безпеки критичної інфраструктури лежить перш за все на національному рівні, а, наприклад, Контртерористичний комітет ООН відносить це завдання до "внутрішньодержавних заходів безпеки".

Як засвідчує Директива Ради 2008/114/ЄС від 8 грудня 2008 р. про ідентифікацію і позначення Європейських важливих інфраструктур та оцінку необхідності вдосконалення їх захисту, основна й остаточна відповідальність за захист об'єктів критичної інфраструктури покладається головним чином на держави-члени та власників (операторів) таких інфраструктур.

Однак загрози інфраструктурі за визначенням включають транскордонні і транснаціональні катаклізми й атаки. У глобалізованому світі нові системи інформації і комунікації, енергетики і транспорту є частиною більш широких міжнародних мереж. Це посилює зацікавленість держав і бізнес-спільноти в здійсненні міжнародного співробітництва щодо захисту транснаціональної критичної інфраструктури від загальних загроз, незважаючи на ряд перешкод і обмежень для такого співробітництва. Серед них, наприклад, – об'єктивні відмінності в технологічному потенціалі і ресурсах зацікавлених сторін, у принципах функціонування різних національних систем безпеки критичної інфраструктури тощо.

Одна з таких відмінностей полягає в різному співвідношенні контролю над критичною інфраструктурою з боку держави і приватного бізнесу в різних країнах. Наприклад, у постіндустріальних країнах Заходу специфіка завдання полягає в необхідності гарантувати безпеку в значній мірі децентралізованих систем, що перебувають під управлінням і у власності приватного сектора. Так, у США до 85 % всіх систем критичної інфраструктури перебуває в приватних руках, а державний Департамент внутрішньої безпеки відповідає лише за 5 з її 13 секторів. В інших країнах, наприклад у Китаї, велика частина критичної інфраструктури перебуває під прямим контролем держави, що відіграє головну роль у забезпеченні її безпеки. Цікаво також, що, наприклад, менша залежність ряду країн, які розвиваються, від високотехнологічних систем управління інфраструктурою і зосередження її значної частини під контролем держави парадоксальним чином у чомусь навіть робить їх менш вразливими перед погрозами нового типу. Це, втім, слабо компенсує такі хронічні проблеми критичної інфраструктури в цих державах, як її громіздкий і неадаптивний характер, зношеність, дефіцит у фінансуванні.

Зростання уваги до терактів як загроз безпеці критичної інфраструктури може допомогти прояснити саме поняття "критичність" у сучасному світі і виявити найбільш "критичні" інфраструктури, які потребують пріоритетної уваги й інвестицій в їх безпеку. Так загроза тероризму диктує необхідність у першу чергу зосередитися на підвищенні безпеки таких вузлів і систем:

- які не тільки схильні до прямого збитку від теракту і вторинного дестабілізаційного впливу, але й у разі захоплення терористами можуть бути самі використані для ударів по інших цілях;

- де збільшення рівня безпеки підвищить загальний ефект безпеки і для інших пов'язаних із ними елементів, а також секторів критичної інфраструктури.

Із більш загальних стратегічних напрямів підвищення безпеки критичної інфраструктури відзначимо необхідність переходу від "стратегії декількох загроз" до стратегії захисту та реагування на множинні загрози. Проста заміна "стратегії однієї загрози" "стратегією декількох загроз" автоматично передбачає свідомо недостатню увагу до інших, також і нових та неочікуваних, загроз інфраструктурі. Більше того, необхідно взагалі вийти за рамки підходу, зацикленого лише на статичному "захисті" окремих, найбільш "критичних" об'єктів та інфраструктур від обмеженого спектра відомих загроз, які в основному визначаються за аналогією з попередніми кризами. Заходи цього типу будуть адекватними тільки в контексті загального підвищення стійкості системи інфраструктури до зовнішніх і внутрішніх загроз і ризиків, також і нових та несподіваних (непрогнозованих).

Звичайно, передбачити всі потенційні загрози і ризики просто неможливо. Однак за умов зростаючої складності і взаємозалежності систем інфраструктури і життєзабезпечення, диверсифікації управління і контролю над ними, множинності і неявності ризиків та загроз у постіндустріальну епоху запорука стабільності критичної інфраструктури полягає в досягненні високого рівня її стійкості до будь-яких системних ударів. Це передбачає створення таких систем і механізмів, які володіють зниженою вразливістю і "вбудованою" здатністю адаптуватися до різких змін, включаючи надзвичайні ситуації різних типів – чи то фізична загроза або, наприклад, раптове блокування надходження або доступу до того чи іншого ресурсу. У даному випадку "стійкість" передбачає здатність системи не тільки витримувати масштабний удар, але й швидко відновлюватися, також і в видозміненому вигляді, адаптованому до нових умов.

Підвищити адаптивність і знизити загальну уразливість системи можна шляхом поєднання різних методів і стратегій, наприклад пошуку і досягнення оптимального балансу між:

- здешевленням вартості, зниженням громіздкості і підвищенням гнучкості інфраструктури за рахунок оптимізації управління, адаптивного менеджменту, модернізації систем зв'язку та інформації, більш активного впровадження мережевих елементів, опори на соціально-технічні інновації;

- забезпеченням страхувальних і резервних потужностей, систем зв'язку та управління.

Мережеві, децентралізовані системи зв'язку і комунікацій, побудовані за принципом "від багатьох до багатьох", також нерідко демонструють більшу стійкість в інформаційну епоху, ніж традиційні комунікаційні системи за принципом "від одного до багатьох".

Існують різні приклади критичних інфраструктур, які зберігали досить високий рівень загальної стійкості і здатність до швидкого відновлення, незважаючи на неможливість забезпечити їх повний захист навіть від

основних загроз.

У цілому для підвищення рівня безпеки критичної інфраструктури необхідні і певний ступінь захисту від найбільш вірогідних, очікуваних і типових загроз, і заходи з підвищення загальної стійкості і пристосовності системи, що дозволяють знизити її вразливість перед новими і несподіваними загрозами. Співвідношення заходів цих двох типів може варіюватися від однієї інфраструктури до іншої. Наприклад, на системах громадського транспорту, де легше визначити характер найбільш імовірних, також і терористичних, загроз, основний наголос за визначенням має бути зроблений на комплексі захисних заходів. У той же час, наприклад, у сфері інформаційних технологій, комунікацій, енергетики особливу увагу слід приділяти забезпеченню загальної стійкості системи, її диверсифікації, резервним потужностям і ресурсам. Така збалансована і комбінована стратегія краще відповідатиме сучасним потребам безпеки критичної інфраструктури.

Завдання захисту критичної інфраструктури порушило проблему узагальнення й аналізу необхідної інформації, що зумовило прийняття в США Акта щодо інформації з критичної інфраструктури (Critical Infrastructure Information Act ("CIIA") [5] у 2002 р. Цим законом регулюється питання щодо обміну інформацією з питань оцінки вразливості та загроз інфраструктурі, також і пов'язаних із терористичними загрозами. Закон запроваджує термін "інформація щодо критичної інфраструктури" як інформації, яка зазвичай не перебуває в полі зору суспільства та належить до безпеки функціонування критичної інфраструктури чи захищених систем. Акт визначає урядовий орган – Департамент внутрішньої безпеки – відповідальним за збір, аналіз та поширення інформації з метою вжиття необхідних заходів із захисту критичної інфраструктури. Одночасно законом установлюються вимоги щодо використання такої інформації (запроваджується режим обмеженого доступу) для недопущення зловживань та захисту суб'єктів господарювання (операторів інфраструктури) від поширення вразливої комерційної інформації.

Сьогодні в стратегіях гарантування безпеки критичної інфраструктури розвинених країн домінують два взаємопов'язані підходи. Перший – пов'язаний із визначенням переважного типу (типів) загроз інфраструктурі. Наприклад, у США в останнє десятиліття спостерігався поступовий відхід від "стратегії захисту від однієї загрози", що переважали в перші роки після подій 11 вересня, також і в підходах нового державного Департаменту внутрішньої безпеки, до проблем безпеки критичної інфраструктури. Вона була зациклена на захист від загроз саме терористичного типу на шкоду іншим, набагато більш поширеним загрозам (one-hazard strategy).

Після колапсу мало не всієї критичної інфраструктури в прибережних районах США в результаті нездатності протистояти наслідкам ураганів у 2005 р. уряд США поступово повернувся до стратегії захисту від двох або декількох найбільш імовірних загроз, включаючи великі техногенні аварії. Ця стратегія більш адекватна і давно домінує в країнах ЄС.

Зокрема в Директиві Європейської Комісії № 786 2006 р., згідно з якою до загальноєвропейської критичної інфраструктури відносять ті об'єкти національної критичної інфраструктури країн – членів ЄС, вплив яких, у разі відмови, інциденту або зловмисного втручання поширюватиметься як на країну, де такий об'єкт розташований, так і на хоча б одну іншу країну – член ЄС. А Директивою Ради 2008/114/ЄС від 8 грудня 2008 р. про ідентифікацію і позначення Європейських важливих інфраструктур та оцінку необхідності вдосконалення їх захисту [6] запроваджується процедура ідентифікації та позначення європейських критичних інфраструктур, а також спільний підхід до оцінки необхідності вдосконалення захисту таких інфраструктур з метою сприяння захисту людей.

Під "критичною інфраструктурою" ("важливою інфраструктурою" - у перекладі фахівців з Інституту законодавства Верховної Ради України [6]) для цілей цієї Директиви розуміють розташоване в державах-членах майно, систему чи їх частину, що є важливими для підтримання життєво необхідних соціальних функцій, здоров'я, безпеки, економічного чи соціального добробуту людей, а також результатом розладу чи руйнування яких у будь-якій із держав-членів може стати неможливість підтримувати зазначені функції.

До недавнього часу такий базовий підхід до гарантування безпеки критичної інфраструктури був майже виключно зосереджений саме на захисті її конкретних структур, ресурсів і об'єктів від обмеженого числа небезпечних, але в цілому відомих і відносно очікуваних загроз. Відповідна до цього підходу стратегія протидії загрозам і запобігання шкоді інфраструктурі спирається на формальні, централізовані системи командування і контролю, спеціалізовані професійні служби та персонал, "закриті" системи комунікацій з використанням спецзв'язку, міжвідомчу взаємодію і взаємодію з населенням за ієрархічним принципом "від одного до багатьох".

У той же час така стратегія схильна до надмірного впливу або навіть диктується реакцією на останні великі катаклізми (масштабні теракти, руйнівні стихійні лиха або великі техногенні катастрофи). Звичайно, необхідність забезпечити певний ступінь захисту критичної інфраструктури від більш звичних і порівняно добре відомих загроз не викликає сумнівів. Для одних систем інфраструктури (наприклад, громадського транспорту або об'єктів, пов'язаних із хімічними, біологічними, радіологічними і ядерними матеріалами) потреба в такому захисті неминуче буде вищою, ніж для інших. Однак підхід, зосереджений на захисті основних вузлів найбільш "критичної" інфраструктури від декількох знайомих загроз за аналогією з останніми великими надзвичайними ситуаціями, у принципі не може забезпечити захист від майбутніх надзвичайних ситуацій.

У цілому такий "механічний" і "статичний" підхід залишається продуктом індустріального суспільства, його економіки і культури. Він не цілком адекватний викликам постіндустріальної епохи, глобалізації, а також інформаційного суспільства і навряд чи може забезпечити захист від багатьох нових, несподіваних і погано прогнозованих загроз [7].

Втім було б неправильно стверджувати, що в Україні не приділяється увага захисту важливих об'єктів, систем і ресурсів, які зазвичай належать до критичної інфраструктури. В Україні діє низка законодавчих актів, що визначають особливості забезпечення захисту вказаної інфраструктури. Проте за результатами досліджень фахівців Національного інституту стратегічних досліджень можна дійти висновку, що загрози таким об'єктам розглядаються у суто відомчому розрізі.

Відсутній загальний механізм управління захистом і безпекою об'єктів критичної інфраструктури, спостері-

гаються непоодинокі випадки дублювання функцій [1]. Відсутність же спільних підходів та узгодженості дій стосовно проблем захисту об'єктів критичної інфраструктури веде до розпорошення коштів та сил.

Така ситуація склалася природним чином – кожне відомство бачило певний спектр загроз для підпорядкованих об'єктів і володіло певним набором інструментів та ресурсів для гарантування безпеки даних об'єктів. В Україні захист об'єктів, які згідно зі світовою практикою належать до категорії "критична інфраструктура", регламентується численними нормативно-правовими актами, які мають переважно внутрішньовідомчий характер. Проте про значну кількість нормативно визначених категорій життєво важливих об'єктів і, відповідно, їх переліків, в Україні не здійснено комплексної оцінки ризиків знищення (ушкодження) таких об'єктів. Як уже наголошувалося, у чинному законодавстві досі не визначено термін "критична інфраструктура", хоча в Стратегії національної безпеки, затвердженій Указом Президента України від 26 травня 2015 р. № 287/2015, серед основних напрямів державної політики національної безпеки України названо "забезпечення безпеки критичної інфраструктури", пріоритетами якого визначено комплексне вдосконалення правової основи захисту критичної інфраструктури, створення системи державного управління її безпекою; посилення охорони об'єктів критичної інфраструктури, зокрема енергетичної і транспортної; налагодження співробітництва між суб'єктами захисту критичної інфраструктури, розвиток державно-приватного партнерства у сфері запобігання надзвичайним ситуаціям та реагування на них; розробка та запровадження механізмів обміну інформацією між державними органами, приватним сектором і населенням стосовно загроз критичній інфраструктурі та захисту чутливої інформації у цій сфері; профілактика техногенних аварій та оперативне і адекватне реагування на них, локалізація і мінімізація їх наслідків; розвиток міжнародного співробітництва у цій сфері.

Отже, підсумовуючи, можна дійти таких висновків. Сьогодні критична інфраструктура – це великомасштабні фізичні або віртуальні системи та ресурси, втрата яких може призводити до неусувних наслідків для економіки та політичної стабільності держави, здоров'я населення. До елементів критичної інфраструктури прийнято відносити енергетичні системи, транспортні магістральні мережі, нафто- та газопроводи, системи супутникового зв'язку та життєзабезпечення мегаполісів, служби екстреної допомоги населенню та реагування на надзвичайні ситуації, державні органи влади, високотехнологічні та оборонні підприємства тощо.

Умови надзвичайної ситуації висувають підвищені вимоги до функціонування елементів критичної інфраструктури, створюють специфічні обмеження, які потрібно враховувати при формуванні планів реагування, розроблені математичних моделей, методів та програмних систем підтримки прийняття рішень.

Упроваджувати використання передового зарубіжного досвіду у сфері моделювання ризиків і загроз виникнення надзвичайних ситуацій на об'єктах критичної інфраструктури держави шляхом сприяння міжнародним контактам експертів і фахівців, обміну відкритою інформацією, публікацій аналітичних матеріалів із зазначеного напряму; подальшої гармонізації безпекових підходів на національному рівні з підходами до захисту критичної інфраструктури, прийнятими провідними країнами світу, зокрема країнами – членами ЄС і НАТО.

Поступово вдосконалюючи законодавство у цій сфері, слід визначити перелік об'єктів критичної інфраструктури, прийняти плани підвищення захищеності об'єктів критичної інфраструктури, розробити програми, спрямовані на зниження ризиків і пом'якшення наслідків надзвичайних ситуацій техногенного характеру на об'єктах критичної інфраструктури.

Література

1. Бірюков Д.С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Д.С. Бірюков, С.І. Кондратов. – К. НІСД, 2012.– 96 с.

2. Бірюков Д.С. Актуальні питання захисту критично важливої для життєдіяльності держави інфраструктури / Д.С.Бірюков С.І.Кондратов // Стратегічні пріоритети. – К.: НІСД, 2012. – Вип. №3(24). – С. 107–113.

3. Хлонь С.Є. Кореляція процесів захисту критичної інфраструктури та підготовки території держави до оборони / С.Є. Хлонь, В.І. Пеньковський, О.Л. Глушкевич, О.В.Устименко // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. – 2014. – № 2(51). – С. 51-56.

4. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT ACT) ACT OF 2001 [Електронний ресурс]. – Режим доступу: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm

5. Critical Infrastructure Information Act of 2002 ("CIIA"). [Електронний ресурс]. – Режим доступу: https://www.fas.org/sgp/crs/RL31762.pdf.

European Programme for Critical Infrastructure Protection – [Електронний ресурс]. – Режим доступу: http://europa.eu/legislation_summaries/justice_freedom_security/fight _against_terrorism/l33260_en.htm

6. Реферативний огляд європейського права / За заг. ред. В.О. Зайчука. – Вип. 12. – К., 2009. – 100 с.

7. Perelman L. J. Shifting Security Paradigms: Toward Resilience // Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience. - Wash., 2007. – P. 26.

Курбанов Я.Л.,
аспірант ОДУВС
Надійшла до редакції: 18.11.2015